

REMARKS

The present invention is a method of authenticating a user agent to a server using session initiation protocol messages and a program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform a method of authenticating a user agent to a server using session initiation protocol messages. In accordance with embodiments of the invention, a method of authenticating a user agent to a server using session initiation protocol messages includes forwarding a SIP request from the UA to a server which may be a CSCF or a PCSCF; forwarding a request for authentication from the server to the UA in response to the SIP request which may be a SIP 401 unauthorized message or a SIP 407 proxy authentication request with the request for authentication including information that the authentication will be performed using a Universal Mobile Telecommunications System (UMTS) Authentication and Key Agreement (AKA) mechanism; forwarding an authentication response from a user agent to the server in response to the request for authentication in accordance with the UMTS AKA mechanism which may be a SIP Register (authorization field) or a SIP Invite (proxy - authorization) and performing an invoked SIP procedure on the server in response to the SIP request if the authentication is deemed successful in view of the authentication response which may be a SIP 200 OK message of the call set up. A field within the authentication response comprises RES (response) and AUTS (synchronization failure parameter) and a field in the request for authentication comprises AUTN (authentication token) and RAND (random challenge).

The objection to the informality in the drawings is noted. However, it is requested that the Examiner indicate if he has in his file the June 5, 2001 Submission of Formal Drawings which shows the "401 unauthorized" message with correct spelling.

Claims 1-16 stand rejected under 35 USC §103 as being unpatentable over SIP, IETF RFC 2543 March 1999 (Handley) in view of 3G TS 33.102 and U.S. Patent 6,477,644 (Turnen). These grounds of rejection are traversed for the following reasons.

Independent claims 1 and 9 have been amended to recite that the Request for Authentication contains a field comprising AUTN (authentication token) and RAND (random challenge) and the authentication response contains a field comprising RES (response) and AUTS (synchronization failure parameter). This subject matter is based upon the subject matter of canceled claims 4 and 12 and pending claims 6 and 14 which have been amended. The subject matter is supported on page 6, lines 3-17 which refer to AUTN and RAND being in the WW-Authenticate Header Field and RES and AUTS being in the authorization header field.

The Examiner's rejection of claims 1-16 is traversed with respect to amended claims 1 and 9 for the following reasons. Handley describe HTTP-digest base authentication for SIP and refer to PGP as being a new scheme defined in RFCC 2015. Handley does not disclose that UMTS AKA or other SIM/USIM based authentication may be used. The Examiner recognizes this by stating that Handley does not explicitly disclose the authentication associated with mobile systems listed as follows:

a: The authentication perform using a universal mobile telecommunication system (UMTS) Authentication and Key Agreement (AKA) mechanism.

The Examiner's reliance on 3GPP TS 33.102 is misplaced. It is noted that the Examiner has referred to Section 6.3.3 and Figure 8 as the basis for modifying Handley with further consideration with Turunen to arrive at the subject matter of the claims. However, Section 6.3.3 discloses a process for authentication of the user to establish a new pair of ciphered integrity keys between VLR/SGSN and the USIM using 3GPP specific protocols. However, a person of ordinary skill in the art understands that SIP as an application layer protocol that is useful outside the 3 GPP environment which has advantages relative thereto. However, there is no reference to SIP or non-3GPP specific protocols.

It should be noted that independent claims 1 and 9 recite substantively authenticating a user agent to a server using session initiation protocol (SIP messages), comprising forwarding a SIP request for the user agent to the server.

It is submitted that a person of ordinary skill in the art would not consider the communications of 6.3.3 of the 3G TS 33.102 for authenticating a user and establishing a pair of ciphered integrity keys between a PLR/SGSN and a USIM to suggest modifying Handley to arrive at the subject matter of the independent claims. The Examiner has not demonstrated any basis in the record why a person of ordinary skill in the art would be led to modify the teachings of Hanley to arrive at the subject matter of the independent claims as amended.

Claim 5 further limits claim 3 in reciting wherein RAND and AUTN vectors are included in a SIP WWW-Authenticate or a Proxy-Authenticate response header field and further claim 13 further limits the storage device of claim 11 wherein RAND and AUTN vectors are included in a SIP WWW-Authenticate or a Proxy Authenticate Response Header Field. This subject matter is not suggested by the proposed combination of Hadley and 3G TS 33.102.

Furthermore, dependent claims 7 and 15 further limit claims 6 and 14 in reciting that the authentication response is included in a SIP authorization or proxy-Authorization Header Field. It is submitted this subject matter is also not suggested by the proposed combination of Hadley and 3G TS 33.102 or Turunen.

It is noted that the Examiner has referred to Turunen as disclosing a corporate user will have the opportunity to make wireless voice and data calls from a mobile terminal via corporate LAN to gain internet access from the mobile host store terminals with the Examiner citing column 1, lines 36-40 and 65-67, and further disclosing the security problem that the Internet is not a secure network and it is possible for a third party to intercept Internet traffic with the Examiner relying upon column 3, lines 34-36, and teaching a method to improve security to allocate new authentication/encryption keys to a mobile host whenever a mobile host makes a new Internet access request with the Examiner relying on column 3, lines 43-46. However, it is submitted that a person of ordinary skill in the art would not consider the aforementioned statements in Turunen to provide sufficient motivation to modify Handley in

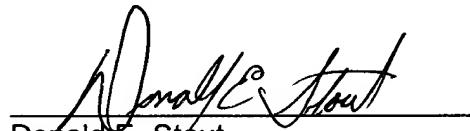
view of 3G TS 33.102 to arrive at the subject matter of the independent claims or claims dependent therefrom.

Newly submitted claims 17-42 have been added to claim further aspects of the further invention which are not rendered obvious by the proposed combination of Hadley, 3G TS 33.102 and Turenen.

In view of the foregoing amendments and remarks it is submitted that each of the claims in the application is in condition for allowance. Accordingly, early allowance thereof is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR §1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 01-2135 (Case No. 0172.38841X00) and please credit any excess fees to such deposit account.

Respectfully submitted,



Donald E. Stout
Registration No. 26,422
ANTONELLI, TERRY, STOUT & KRAUS, LLP

DES/vvr

Attachments